UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 09-10243-MLW
	)	
RYAN HARRIS	)	

> "The broad language of the mail and wire fraud statutes are both their blessing and their curse. They can address new forms of serious crime that fail to fall within more specific legislation. On the other hand, they might be used to prosecute kinds of behavior that, albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected by the instigators to form the basis of a federal felony. . . . Finally, we caution that the wire fraud statute must not serve as a vehicle for prosecuting only those citizens whose views run against the tide, no matter how incorrect or uncivilized such views are."
>
> United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997).

DEFENDANT'S MEMORANDUM IN SUPPORT OF MOTION TO DISMISS SUPERSEDING INDICTMENT FOR LACK OF VENUE AND ON THE MERITS; ALTERNATIVELY FOR TRANSFER TO ANOTHER DISTRICT

Defendant, Ryan Harris, respectfully submits this memorandum in support of his motion, pursuant to Fed. R. Crim. P. 12 and 18, to dismiss the Superseding Indictment ("Sup. Ind.") for lack of venue in the District of Massachusetts. As grounds, he states, inter alia, that the government's attempt to create venue in this District over an out-of-state product seller for the actions of product users fails as a matter of law. For the same reasons, Harris moves to dismiss the indictment outright, as well as for violation of the Due Process Clause of the Constitution.

Alternatively, Harris moves, pursuant to Fed. R. Crim. P. 21(b), for a transfer to the United States District Court for the Eastern District of California in the interest of justice. The government has disclosed its intention to commence in that District criminal proceedings against Harris for tax offenses relating to this charged conduct.

I. PROCEDURAL HISTORY AND SUMMARY OF ARGUMENT

A. Procedural History to Date

Harris and corporate defendant TCNISO, Inc. were initially charged by indictment in six counts: count one charged conspiracy to commit computer fraud and wire fraud in violation of 18 U.S.C. § 371; count two charged aiding and abetting computer fraud pursuant to 18 U.S.C. §§ 2, 1030; and counts three to six charged aiding and abetting wire fraud of a single user, under 18 U.S.C. §§ 2, 1343.

On January 24, 2011, Harris filed a motion seeking dismissal of the case for want of venue, and, alternatively, seeking transfer under Fed. R. Crim. P. 21(b). Dkt. #38. On February 8, 2011, the government filed its response to this motion. Dkt #42.

On February 23, 2011, the government dismissed the indictment against the corporate defendant TCNISO, Inc., on the grounds it was defunct and not represented by counsel. Dkt. #43.

On May 18, 2011, the government filed an eleven-count Superseding Indictment with Harris as lone defendant. Dkt #46. The Superseding Indictment narrowed the case against Harris by

abandoning the computer fraud charges arising under 18 U.S.C. § 1030(a)(4), and by charging only theories of wire fraud pursuant to 18 U.S.C. § 1343.

B. The Superseding Indictment

The Superseding Indictment alleges that Harris was the "founder, owner, and president of, and software developer for" a company called TCNISO. Sup. Ind. at ¶ 1. TCNISO developed and distributed "'cable modem hacking' software and hardware" that were "designed to modify cable modems so that users could obtain internet service from Internet Service Providers, without paying for this service and without disclosing their true identities." Id.

Count one of the Superseding Indictment charges Harris with conspiracy under 18 U.S.C. § 371 to commit wire fraud in violation of 18 U.S.C. §1343 by aiding four individuals and other unnamed "users" to obtain free internet service. Counts two through eleven charge Harris with aiding and abetting wire fraud in violation of 18 U.S.C. §§ 1343 and 2, by aiding four named users of TCNISO products in obtaining free internet access.

C. Summary of Argument

The government does not charge that TCNISO's products as designed violated federal law, nor would venue exist in this District for such a claim. Instead, the government asserts that the products as used violated federal law, that Harris knew that downstream users utilized his "products and service to obtain

internet service and faster internet access without paying." Sup. Ind. at ¶ 26. Harris is charged criminally under theories of secondary liability with the conduct of product users.

Alleging secondary liability to bootstrap venue in this District poses significant pleading problems. Secondary liability presumes primary culpability. However, a product seller is not, without more, complicit in a conspiracy with a product user. The existence of some complicitous "more" might create conspiratorial culpability with the user, but the pleadings do not include such allegations.

The pleadings in this case are novel,[1] even audacious, and must be so since they are drafted to achieve venue based solely on the remote conduct of individual customers. Ordinarily, a claim to venue follows from the identification of a chargeable offense. Here, however, the decision to seek venue in this District came first, occasioning pleadings which run afoul of legal boundaries and which fairly beg for pretrial contest.

Finally, there remains the issue of the appropriateness of the government's use of the wire fraud statute to address a

[1]In a case filed in the Southern District of New York on January 28, 2010, United States v. Matthew Delorey, 10 Cr. 00682, the government charged a supplier of modified modems with wire fraud, but later reduced the charge to a misdemeanor of unlawful access under 18 U.S.C. § 1030(a)(6). In an earlier case brought in the Southern District, United States v. Thomas Swingler, Cr. 09MJ0033,the government charged a modem seller with access device fraud under 18 U.S.C. § 1029(a)(3) and (b)(2), but dismissed the charge.

firmware developer's responsibility for a customer's theft of cable service. Aggressive use of the wire fraud statute is a characteristic of this District. An example is United States v. LaMacchia, 871 F.Supp. 535 (D.Mass. 1994), where the court rejected the government's invocation of the statute to reach the unauthorized, non-commercial distribution of copyrighted software over the internet. Similarly, in United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997), the First Circuit reversed a wire fraud conviction for an IRS employee who browsed through IRS files but did not send or obtain any information. The First Circuit criticized the aggressive use of wire fraud to criminalize behavior involving electronic, computer based access to information. Id. at 1079 ("The broad language of the mail and wire fraud statutes are both their blessing and their curse.").

II. THE FIRMWARE AND ITS USERS

A. Government's Accusations about the Firmware[2]

"In order to access the internet through a cable network, a subscriber installs a cable modem, which connects the subscriber's computer to the ISP's cable network." Sup. Ind. ¶9. All modems have an individual identifier called a media access control (a "MAC address"). When a modem is connected to a cable belonging to an ISP, the modem sends its MAC address to the ISP. If the ISP recognizes the MAC address as belonging to a

[2]The following section draws on material received from the government during discovery. Harris recites these facts to orient the Court and does not mean to endorse them as true or correct.

subscriber's modem, the ISP will allow that modem to access the internet. This access will be provided at the speed the owner of the modem has purchased. If the ISP does not recognize the MAC address, it will not allow the modem to access the internet.

According to the government, TCNISO's products and website allowed individuals to shortcut the usual procedures. Allegedly, one TCNISO product, called Blackcat, was a combination of hardware, including a modem and software called Sigma, which enhanced end-users' capability, but which the government alleges permitted an individual to change his or her modem's MAC address (also called "spoofing") and thereby receive faster service than he or she had paid for, or completely free internet access. The government notes that spoofing also allowed people to mask their identities while browsing the internet. Allegedly, TCNISO products also allowed ISP subscribers to receive faster service than they purchased by changing the configuration files on their modems, which are the values assigned to modems by ISP corresponding with the speed of service purchased.

In addition to products like Blackcat, the government alleges that TCNISO made a product called Coaxthief that enabled individuals to find (or "sniff") the MAC addresses of other modems. The government asserts that the TCNISO website included a forum on which TCNISO users traded MAC addresses and discussed their experiences and problems with using the products to get faster or free internet.

B. Product Users

The indictment identifies four users and two affected ISPs, but is framed more broadly. In response to a discovery letter dated May 17, 2010, the government claims intrusions into no fewer than 22 ISPs, and states that this number may increase as investigation continues. The government asserts that there are too many dates of user access to detail: "Because many of the TCNISO customers who used the company's products to access ISPs' networks without authorization did so on a regular basis, we cannot identify the dates of all of these accesses." Discovery Ltr., May 17, 2010. Indeed, except for the four named users, the government has provided no identifying details regarding "users" and their alleged activities. Moreover, the word "user" appears to include all who acquired TCNISO products, even non-customers; so actions by non-customers, on the government's charging theory, can trigger secondary criminal liability for Harris.

C. Allegations Specific to Massachusetts

The indictment alleges two links to this District. The first relates to the four identified "users," N.H.,[3] W.M., L.G., and J.L., all of whom allegedly used TCNISO products to access the internet without paying. The indictment states that W.M., L.G., and J.L. purchased these products through the TCNISO website, but there are serious questions about where N.H.

[3]N.H. was identified by his online moniker, DShocker, in previous pleadings.

obtained the products that he used.[4] Each user allegedly visited the TCNISO forums to get information about changing their MAC addresses and configuration files. N.H. is the only user who is alleged to have communicated directly with Harris beyond ordering products. The indictment implies that all of these activities were performed in Massachusetts.

The second alleged link is government-generated. In late 2008, an FBI agent in Boston, Massachusetts accessed the TCNISO website and bought five modems and a copy of Harris's book, Hacking the Cable Modem. To complete this purchase, the agent called TCNISO in California, and spoke with someone named "Ryan." The agent subsequently received the modems and book in Massachusetts. According to the indictment, "[t]hese modems were capable of obtaining free and faster internet service from a cable network." Sup. Ind. at ¶ 58.

Apart from the named users and the FBI agent, none of the entities and individuals mentioned in the indictment reside in or are alleged to have entered Massachusetts at any time. According to the indictment, I.L., an unindicted co-conspirator who worked as a software developer for TCNISO, resided in Kentucky; and C.P., an unindicted co-conspirator who was once the vice-

[4]N.H.'s Grand Jury testimony indicates that he got a modem that he planned to use to get free internet access "from somebody on another website." Grand Jury Testimony, May 6, 2009, Bates Harris 208. He also testified that some of the software he used to gain free internet access did not come "directly from TCN[ISO], but it was from somebody who had gotten it from TCN[ISO]." Id. at Harris 221.

president of TCNISO, lived in California. None of these individuals is alleged to have entered or to have specifically sought contact with anyone in Massachusetts.

D. The Reality of the Modems

The Superseding Indictment implies, but does not affirm, that the sole purpose of TCNISO's products was to enable individuals to get free or faster internet service. It also suggests, but again does not affirm, that when an individual received products from TCNISO, the products were already configured such that once plugged in, the user could obtain free or faster access. The government cannot prove either of these suggestions, as neither is supported by fact. The products that TCNISO developed and distributed had multiple capabilities, including to permit routine connections to an ISP.

When developers design software and hardware, they typically program them in a way that prevents users from accessing some of the product's functionality. See In re Synchronoss Securities Litigation, 705 F. Supp. 2d 367, 375 (D.N.J. 2010) (noting that "many smartphone manufacturers 'lock' the devices" and that many smartphone users "want to gain control over the applications/software they can install on their mobile devices," which can be done via jailbreaking). Sophisticated users, however, often want more control so they can increase the product's functionality. Id.; see also Meinrath, Sascha, et. al, Digital Feudalism, 19 CommLaw Conspectus 423, 461-62 (2011)

(discussing benefits of opening internal workings of devices to users). Revealing the internal workings of hardware and software is called "jailbreaking." See 75 Fed. Reg. 43825-01, 43828-30(2010) (Copyright Office regulations permitting jailbreaking of smartphones). In addition to adding functionality, sophisticated users may try to open devices to show that they can, the programming equivalent of a crossword puzzle. One recent, well-known iteration of jailbreaking involves the iPhone; sophisticated users gained access to the internal coding of the machine so that it could be used in ways that Apple's manufacturing techniques otherwise blocked. See id.

What TCNISO did was to jailbreak modems; to open the internal workings and inherent possibilities of the modem to the user. After this process, the modems still operated as normal modems, but an opened modem also allowed sophisticated users to do things they could not do with a closed modem. Revealing the functions of the modem enabled users to change MAC addresses and configuration files, but that was not the sole purpose of the modems.

When users obtained a modem from TCNISO, they received a typical modem with increased potential, which was theirs to explore. The modem they received could be plugged in and used as a modem immediately, but accessing the revealed potential of the modem required additional work by the user. Whether the user wanted to diagnose a network problem or attempt to obtain faster

service, that user would have to go through a number of steps, some of which are complicated and required advanced computer knowledge.

III. THE CLAIM TO VENUE

The Superseding Indictment alleges that four named Massachusetts residents used products developed by Harris to obtain free internet access. There are no allegations that Harris had personal contact with three of these individuals. Nor does the government allege that any of these users told Harris what he or she planned to do with the TCNISO products.

The government's pleading presumes, incorrectly, the existence of two critical legal predicates: (a) that a seller of a product conspires with, and aids and abets, his users, and (b) that the actions of an individual user can be linked into a conspiracy joining all users. Neither proposition is supported in the law, but both are conditions precedent to the viability of this action, as a matter of venue and as a matter of pleading.

A. Venue Generally and Pre-Trial Resolution of the Issue

When a defendant challenges the government's choice of venue, "the government must prove by a preponderance of the evidence that venue is proper as to each individual count." United States v. Salinas, 373 F.3d 161, 163 (1st Cir. 2004). Generally, venue is proper if the district of the trial is a district in which the crime charged occurred.

The constitutional limits on venue in criminal cases derive from two provisions of the Constitution and from the Federal Rules of Criminal Procedure. See United States v. Cabrales, 524 U.S. 1, 6 (1998) (delineating law governing choice of venue); Salinas, 373 F.3d at 164. Article III requires that criminal trials "shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. The Sixth Amendment further specifies that "[i]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." U.S. Const. amend. 6. Rule 18 of the Federal Rules of Criminal Procedure codifies the constitutional command, stating that "the government must prosecute an offense in a district where the offense was committed." Fed. R. Crim. P. 18.

The "'locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it.'" Salinas, 373 F.3d at 164 (quoting United States v. Anderson, 328 U.S. 699, 703 (1946)). Although the statute's action verbs are not the sole consideration, a court "must begin by 'identify[ing] the conduct constituting the offense (the nature of the crime) and then discern the location of the commission of the criminal acts.'" Id. (quoting United States v. Rodriguez-Moreno, 526 U.S. 275, 279 (1999)).

Here, the locus of the crime is complicated by the pleading liberties taken by the government. Ordinarily, venue follows from an allegedly criminal act. Not so here, where the government started with venue and then reverse engineered the crime. Only this reversal can explain the oddity of the pleadings, where the "crime" is alleged complicity in the downstream conduct of product users.

To evaluate the claim to venue, this Court may make a threshold evaluation of the legal claims and attendant factual claims. This is also true in connection with an inquiry whether outright dismissal is in order. Fed. R. Crim. P. 12 "encourage[s] district courts to entertain and dispose of pretrial criminal motions before trial if they are capable of determination without trial of the general issues." United States v. Levin, 973 F.2d 463, 467 (6th Cir. 1992); see also Fed. R. Crim. P. 12(b), advisory committee's note on subdivision (b)(1) and (2); United States v. Grimmett, 150 F.3d 958, 961 (8th Cir. 1998); United States v. Hall, 20 F.3d 1084, 1086-87 (10th Cir. 1994); United States v. Risk, 843 F.2d 1059, 1061 (7th Cir. 1988); United States v. Brown, 925 F.2d 1301, 1304-05 (10th Cir. 1991). Cf. United States v. Hristov, 2011 WL 1443348 (D. Mass. 2011) (noting that pretrial resolution of "threshold" legal issues may be proper even if pretrial ruling on the merits is not). While a facially valid indictment returned by a duly constituted grand jury usually calls for a trial on the merits,

see Costello v. United States, 350 U.S. 359, 363 (1956), Rule 12 permits the Court to determine whether the government can prove its case beyond a reasonable doubt. To resolve these pretrial motions, the court "may make preliminary findings of fact necessary to decide the questions of law presented by the pre-trial motion so long as the court's findings on the motion do not invade the province of the ultimate finder of fact." United States v. Jones, 542 F.2d 661, 664 (6th Cir. 1976); see also United States v. Covington, 395 U.S. 57, 60 (1969).

B. Venue Based on Secondary Liability Is Not Proper in Massachusetts Because a Product Manufacturer is Not an Aider and Abettor of the Product User

To prove that Harris aided and abetted product users, the government must establish that he intended to aid and abet them and knew that he was aiding and abetting them.

In United States v. Peoni, the defendant sold counterfeit currency to someone who sold it to a third party. 100 F.2d 401, 401-02 (2nd Cir. 1938). The court ruled that Peoni could not be an accomplice to, or in a conspiracy with, the third party's crime of possession. Id. at 402-03. In his opinion, Judge Learned Hand noted the difference between the scope of criminal and civil liability.

> The prosecution's argument is that, as Peoni put the bills in circulation and knew that Regno would be likely, not to pass them himself, but to sell them to another guilty possessor, the possession of the second buyer was a natural consequence of Peoni's original act, with which he might be charged. If this were a

> civil case, that would be true; an innocent buyer from Dorsey could sue Peoni and get judgment against him for his loss. But the rule of criminal liability is not the same; since Dorsey's possession was not de facto Peoni's, and since Dorsey was not Peoni's agent, Peoni can be liable only as an accessory to Dorsey's act of possession.

Id. at 402. Accessorial liability requires that the alleged accessory "in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed." Id.; see also United States v. Medina-Roman, 376 F.3d 1, 3 (1st Cir. 2004).

In fraud cases, the government must prove that the defendant willfully participated "in [the] scheme with knowledge of its fraudulent nature and with intent that these illicit objectives be achieved." United States v. Urciuoli, 513 F.3d 290, 300 (1st Cir. 2008) (internal quotation marks omitted). The First Circuit explained this mens rea requirement in a mail fraud case where the defendant's role in the alleged conduct was helping to dismantle a brand-new car:

> In order to sustain a conviction in the instant case, the government must show that the defendant, Paul Loder, consciously shared in the specific criminal intent of the principals, the Morrisons, to commit mail fraud. In other words, the government must present evidence that would allow a rational trier of fact to conclude that Loder had knowledge that he was furthering mail fraud. Although he need not be aware of all the details of the mail fraud, a general suspicion on Loder's part that his participation in dismantling the Caprice was "for some nefarious purpose" is not enough to make him guilty of aiding and abetting mail fraud.

United States v. Loder, 23 F.3d 586, 591 (1st Cir. 1994). The court cited with approval United States v. Barclay, 560 F.2d 812 (7th Cir. 1977), where the court reversed a conviction for bank fraud and abetting bank fraud because the trial judge's instructions permitted the defendant to be convicted without finding that he knew that the principal was going to make a false entry with the specific intent to defraud the bank, and without finding that the defendant shared the principal's specific intent to defraud the bank. Accomplice liability requires that the defendant have the same mens rea as the principal, in this case, specific intent to achieve an illicit objective. See United States v. Serrano, 870 F.2d 1, 6 (1st Cir. 1989).

The government cannot prove that Harris had knowledge of the individual purchasers' motives or that Harris intended to aid them in achieving the results they chose. The government does not allege any personal contact between Harris and the named users that would establish that he had the intent to help each one of them in his or her own personal quest to get free internet service.

The government's pleading simply presumes legal culpability from product capability. In doing so, the government abandons well-developed legal doctrines of criminal liability. Its approach more closely mimics the civil notion of contributory liability than any theory of criminal liability. Illustrative is MGM Studios, Inc. v. Grokster, 545 U.S. 913 (2005), where

copyright holders sued Grokster alleging that its software was intended to allow users to download copyrighted works. The Supreme Court endorsed the availability of theories of contributory and vicarious liability to permit indirect civil liability. Id. at 929-30. Akin to the Grokster approach, the government here foregoes suit against direct cable trespassers in favor of proceeding against Harris. But in doing so, it eviscerates long-honored legal boundaries by recasting as criminal a civil legal theory. It does so, transparently, to engineer venue in this District. To invoke Judge Hand: "the rule of criminal liability is not the same [as civil]." Peoni, 100 F.2d at 402.

C. Venue Based on Secondary Liability Is Not Proper in Massachusetts Because a Product Manufacturer is Not in a Conspiracy With the Product User

The government also attempts to create venue in this District by joining Harris in an overarching conspiracy with all users of TCNISO products, including the named users in Massachusetts.

To establish a conspiracy, the government must prove that "'each defendant knowingly and voluntarily agreed with others to commit a particular crime.'" United States v. Rivera-Rodriguez, 617 F.3d 581, 596 (1st Cir. 2010) (emphasis added) (quoting United States v. Rivera Calderon, 578 F.3d 78, 88-89 (1st Cir. 2009)). The government must establish that the defendant had the

"intent to agree and intent to commit the substantive offense." Id. (quoting United States v. Bristol-Martir, 570 F.3d 29, 39 (1st Cir. 2009)).

"[A] buyer-seller relationship, simpliciter, is an insufficient predicate for finding that the buyer and seller are guilty as coconspirators." United States v. Santiago, 83 F.3d 20, 23-24 (1st Cir. 1996)(emphasis in original); see also United States v. Moran, 984 F.2d 1299, 1302-03 (1st Cir. 1993); United States v. Gee, 226 F.3d 885, 895 (7th Cir. 2000) (noting, in case involving defendants accused of selling modules that could enable cable converter boxes to receive free television service, that a "mere buyer-seller relationship" is not a conspiracy). A buyer-seller relationship is only a conspiracy if the seller has "clear, not equivocal" knowledge of the conspiracy and intended to join it. Direct Sales Co. v. United States, 319, U.S. 703, 711 (1943).[5]

In Direct Sales, the Court affirmed a conviction of a registered drug manufacturer for the sale of restricted drugs to a small-town physician. The Court pointedly noted that the narcotic at issue (morphine sulphate) was "restricted," that is, "incapable of further legal use except by compliance with rigid

[5] The government asserts that Direct Sales supports venue in this case because the defendant operated a mail order business in New York, and was convicted of conspiracy in South Carolina based on shipments he made to that state. However, Direct Sales was not a venue contest. Moreover, it involved sales of controlled substances, repeatedly and in great quantities, making it quite unlike the single-sale circumstances here.

regulations [regarding distribution]." This character of the commodity "ma[de] a difference in the quantity of proof required to show knowledge that the buyer will utilize the article unlawfully." Id. at 710-11. Nonetheless, the Court stated that the "inference of such knowledge [of a conspiracy] cannot be drawn merely from knowledge the buyer will use the goods illegally." Id. at 709. Nor does "the act of supplying itself" demonstrate "an agreement or concert of action between the buyer and the seller amounting to conspiracy." Id. To prove a conspiracy, the government must show that, "by the sale, [the seller] intends to further, promote, and cooperate in [the buyer's intended illegal use]." Id. at 711. "[N]ot every instance of sale of restricted goods, harmful as are opiates, in which the seller knows the buyer intends to use them unlawfully, will support a charge of conspiracy." Id. at 712. The Supreme Court noted:

> [That facts do not support a charge of conspiracy] may be true, for instance, of single or casual transactions, not amounting to a course of business, regular, sustained and prolonged, and involving nothing more on the seller's part than indifference to the buyer's illegal purpose and passive acquiescence in his desire to purchase, for whatever end. A considerable degree of carelessness coupled with casual transactions is tolerable outside the boundary of conspiracy. There may be also a fairly broad latitude of immunity for a more continuous course of sales, made either with strong suspicion of the buyer's wrongful use or with knowledge, but without stimulation or active incitement to purchase.

Id. at 712, n.8.

Because a conspiracy is an agreement to commit a particular crime, the defendant must know and intend the specific criminal objective at the heart of the conspiracy. Rivera-Rodriguez, 617 F.3d at 596; see also United States v. United States Gypsum Co., 438 U.S. 422, 443 n.20 (1978); United States v. Ortiz, 447 F.3d 28, 32-33 (1st Cir. 2006). To be convicted as a conspirator, an individual must know the conspiracy's "essential features and general aims." United States v. Stubbert, 655 F.2d 453, 456 (1st Cir. 1981).

The government cannot prove that Harris knew of a conspiracy, intended to join a conspiracy, or intended to commit a particular crime. "[I]ndifference to the buyer's illegal purpose," alone is insufficient. Direct Sales, 319 U.S. at 713, n.8. Moreover, the products here were not legally restricted. Even in narcotics cases, courts will not infer a conspiracy when a seller makes a one-time sale or multiple "casual" sales with no indication of commitment to the buyer. See e.g. Moran, 984 F.2d at 1302-03; United States v. Izzi, 613 F.2d 1205, 1210 (1st Cir. 1980); United States v. Thomas, 284, F.3d 746, 751-54 (7th Cir. 2002); United States v. Gore, 154 F.3d 34, 40-41 (2d. Cir. 1998); United States v. Mancari, 875 F.2d 103, 105 (7th Cir. 1989).

Even assuming that Harris knew that the product he distributed was going to be used illegally, that does not mean that he knew of any conspiracy. United States v. Falcone, 311 U.S. 205, 208-10 (1940); see also Direct Sales, 319 U.S. at 709.

Similarly, even if "[i]t is a fair inference that defendant knew what was going on . . . that is not enough to establish intent to conspire." United States v. Ocampo, 964 F.2d 80, 82 (1st Cir. 1992); see also United States v. Morillo, 158 F.3d 18, 23 (1st Cir. 1998). The government has failed to allege anything more here, and cannot establish Harris's "informed and interested cooperation, stimulation and instigation" in any conspiracy. Direct Sales, 319 U.S. at 713; see also United States v. Zambrano, 776 F.2d 1091, 1095 (2d. Cir. 1985).

Because the government cannot establish that Harris knew of, intended to join, or aided a conspiracy to commit a particular crime, allegations that he was part of such a conspiracy cannot be used to import venue into this District.

D. The Government Cannot Establish a Single Conspiracy

The government has charged a single overarching conspiracy involving Harris, two TCNISO employees, and four alleged product users. This agglomeration of alleged co-conspirators does not establish a single conspiracy.

The measure of a conspiracy is the scope of the agreement upon which the conspiracy is founded, and one agreement and conspiracy can encompass many substantive offenses. Braverman v. United States, 317 U.S. 49, 53-54 (1942). "A single agreement to commit several crimes constitutes one conspiracy. By the same reasoning, multiple agreements to commit separate crimes

constitute multiple conspiracies." United States v. Broce, 488 U.S. 563, 570-71 (1989). Whether there is a single conspiracy depends on the "totality of the circumstances," particularly focusing on the "existence of a common goal, evidence of interdependence among the participants, and the degree to which their roles overlap." United States v. Fenton, 367 F.3d 14, 19 (1st Cir. 2004).

In the present case, the government has alleged a "hub and spoke" conspiracy, with a central core of conspirators but no common cause linking users on the spokes. See Kotteakos v. United States, 328 U.S. 750, 755 (1946). This structure and the factors listed above militate in favor of finding multiple conspiracies, one for each spoke. Id. at 808.

The first factor, a common goal, is an "overall objective to be achieved by multiple actions." United States v. Chandler, 388 F.3d 796, 811 (11th Cir. 2004). Thus, in Kotteakos, multiple individuals seeking to defraud the Federal Housing Administration were not in a single conspiracy despite their links to a central figure, because "the other individuals in each loan transaction had no interest in the success of any loan application other than their own." United States v. Smith, 82 F.3d 1261, 1269-70 (3d Cir. 1996) (explaining Kotteakos). Similarly, in Chandler, multiple conspiracies were found where the government conceded that although each individual was pursuing the same goal of embezzling McDonald's game stamps, no individual "was aware that

it was participating in anything larger than its own redemptions." 388 F.3d at 811.

The government's allegations do not establish that the users of TCNISO products had a single goal. Even if every user desired free internet access, no user had an interest in another's success or failure. Nor did Harris have an interest in the users' success or failure. Indeed, the government's allegations that the users sought access from multiple ISPs across the country, demonstrates that users did not have a common objective.

The second factor, interdependence, exists when "the activities of one aspect of the scheme are necessary or advantageous to the success of another aspect of the scheme." United States v. Portela, 167 F.3d 687, 695 (1st Cir. 1999) (internal quotation marks omitted). The circumstances in this case weigh strongly against finding interdependence. The users accessed diverse ISPs, and were scattered across the country. The only commonality between them was the use of TCNISO's products and website. Nothing indicates that each individual enterprise was necessary or even advantageous to any of the others.

Finally, courts look to the degree to which the alleged co-conspirator's roles overlapped. A conspiracy involving one central figure is, by definition, the minimal amount of overlap possible. Given the above reasoning on commonality and interdependence and cases like Kotteakos, Chandler, and Smith,

one common company is not enough to establish an overarching conspiracy in this case.[6]

Ordinarily, the issue of whether there is one conspiracy or multiple conspiracies is a question of fact. However, the Superseding Indictment fails to state anything that would support its charge of a single mega-conspiracy. Cf., United States v. David, 940 F.2d 722, 732 (1st Cir. 1991). This charging device of one overarching conspiracy is being used to obtain venue and to string together of isolated, non-criminal incidents into some theory of secondary liability. As the Supreme Court warned in Direct Sales, "charges of conspiracy are not to be made out by piling inference upon inference, thus fashioning what, [in Falcone], was called a dragnet to draw in all substantive crimes." 319 U.S. at 711. The government's dragnet in this case seeks not only to draw in disparate crimes, but also to force an improper venue, and it must be examined before trial.

E. The Remaining Contacts with this District Do Not Support Venue

The purchase of modems and a book by an undercover agent located in Massachusetts, does not confer venue. An investigating agent's phone call to a target, made from a location of the agent's choosing on the eve of prosecution, is

[6]According to the facts alleged in the government's indictment, Harris only had personal contact with one of the alleged co-conspirators, N.H., but as mentioned earlier, N.H. never purchased anything from TCNISO. The other alleged co-conspirators may have purchased products from TCNISO, but they did not have any contact with Harris.

not a meaningful measure of the locus of a crime. It is instead an invitation to manipulate venue. TCNISO's actions were taken in California, and no representative of the company is alleged to have come to Massachusetts. Basing venue on this transaction would allow the government to manufacture venue in any district in the country. See United States v. Naranjo, 14 F.3d 145, 147-48 (2nd Cir. 1994) (rejecting defendant's argument that the government had "artificially created venue," but implying that a trial is not proper in a district where the government had "orchestrated" venue).

Aside from the secondary liability theories and the FBI's arranged purchase, nothing ties Harris or this case to Massachusetts. Because the government cannot establish that venue is proper by a preponderance of the evidence, this Court should dismiss the indictment for lack of venue.

IV. THE GOVERNMENT'S CHARGING DECISIONS RAISE ISSUES OF VAGUENESS AND OVERREACHING

This prosecution tests the boundaries of the wire fraud statute itself and raises issues of vagueness.

The void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement. Kolender v. Lawson, 461 U.S. 352, 357 (1983). This doctrine "addresses concerns about (1) fair

notice and (2) arbitrary and discriminatory prosecutions." Skilling v. United States, 130 S.Ct. 2896, 2933 (2010). In Czubinski, the First Circuit warned of potential vagueness problems inherent in the wire fraud statute:

> The broad language of the mail and wire fraud statutes are both their blessing and their curse. They can address new forms of serious crime that fail to fall within more specific legislation. On the other hand, they might be used to prosecute kinds of behavior that, albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected by the instigators to form the basis of a federal felony.

Czubinski, 106 F.3d at 1079 (citation omitted). This case falls into the latter category.

The government alleges three main actions underlying Harris's criminal culpability: he made a product that was capable of intruding into networks; he made a product that was capable of "sniffing" MAC addresses; and he ran an internet forum on which people shared information about obtaining free or faster access.

First, Harris's company sold firmware arguably used by others to obtain enhanced or free service. That it can be used in that fashion does not create culpability. A manufacturer of radar detectors, which serve little purpose other than to embolden drivers to speed, does not face aiding and abetting charges for a resulting vehicular homicide. Contemporary computing platforms and devices, such as Microsoft Windows XP, cell phones, and iPods, automatically detect and connect to unsecured wireless internet networks. These devices are

preprogrammed to find any available wireless network, to exploit vulnerable networks, and to permit non-payers to reach and use residential and business networks. Once could imagine waiting in vain for an indictment of Microsoft on a theory that its design aided its customers to access vulnerable network systems.

Second, MAC addresses function as mailing addresses for electronic devices; electronic devices communicate by exchanging MAC addresses. MAC addresses sent over unencrypted networks are routinely intercepted, for example by companies developing geo-location services. See, e.g., Motion to Dismiss Plaintiff's Consolidated Class Action Complaint, In re Google Inc. Street View Electronics Communications Litigation, No. 5:10-md-02184 JW at 3 (9th Cir. Mar. 21, 2011). Companies such as Google, Microsoft, and Apple use this information to help device users pinpoint their location based on which networks their electronic devices can detect. Id.; see also Leena Rao, Microsoft Taps Navizon to Power Mobile Geolocation, Washington Post, Mar. 2, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030201828.html. Tools that extract data, whether screen scraping (removing text), website scraping (extracting data underlying a website), or website harvesting (extracting data by following links from the website), are common and have been the subject of civil litigation. See, e.g., EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (considering

"scraper" designed to harvest information from one company's website); In re Pharmatrak, Inc., 329 F.3d 9, 13-14 (1st Cir. 2003) (discussing "cookies," packets of information that can be sent from a web server to a web browser, which in this case gathered information about individuals who visited a given website). Providing a means of harvesting MACs is not unlawful.[7]

Third, federal law protects individuals who operate internet forums from liability for the comments of third parties: "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). While the statute should not be construed to "impair the enforcement of ... any Federal criminal statute," § 230(e)(1), it does not require a forum host to interdict communications regarding web addresses or sniffing activities, which are not illegal. Given the massive volume of information communicated online, "[i]t would be impossible for service providers to screen each of their millions of postings for possible problems." Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997). If the "specter of tort liability" would have a "chilling effect" on potential forum operators, surely the possibility of criminal liability would be even more frightening. Id.

[7]See also United States v. Drew, 259 F.R.D. 449 (C.D.Ca. 2009) (accessing a company's server by deceit was not a violation of the Computer Fraud and Abuse Act since merely a violation of the provider's terms of service.)

In each cited instance, whether involving system intrusions, sniffing, or internet forums, the boundaries of permissible internet behavior have been contested in civil proceedings. From Google, to Apple, to Grokster, the internet behavior of companies has been challenged civilly, not criminally, and not at the price of any person's freedom. Not so here, raising the concern voiced by the First Circuit in Czubinski, that "the wire fraud statute must not serve as a vehicle for prosecuting only those citizens whose views run against the tide, no matter how incorrect or uncivilized such views are," (106 F.3d 1069 at 1079). Nor is it clear that the federal wire fraud statute is the appropriate means to prosecute a theft of service claim, typically the stuff of state courts. In this light, it gives pause that cable providers can enlist the formidable prosecutorial power of the United States against a small firmware provider. This is particularly true where Mr. Harris is the only party prosecuted, and where he had the temerity to publish a book called "Hacking the Cable Modem." While large internet players, even rogue ones like Grokster, face civil sanctions, only the truly inconsequential seemingly earn a criminal prosecution.

Which begs the constitutional question whether the wire fraud statute, with its soft boundaries and built-in ambiguities, gives fair notice of possible prosecution. Certainly, no large internet actor has reason to fear the statute's wooly terms might threaten prison for its corporate principals. Certainly, Sony

never feared its VCR technology would generate a criminal infringement action. Nor would telephone providers who deliberately piggy-backed on competitor's phone lines for commercial advantage.[8]

There remains the issue of harm. The government alleges a scheme to defraud and to obtain money and property by means of material false and fraudulent pretenses by individual users. Any financial harm arising under the individual counts for theft of service might be $60 monthly. Even if, as the indictment alleges, three of the named users obtained free internet for about a year, this might lift the sum to $720. The money at issue for trespassing on a cable network is hardly the stuff of wire fraud.

Using the criminal law as a battle ground, selectively and arbitrarily, to litigate Harris's responsibility as a firmware seller for product use by customers, as well as to delineate the boundaries of the definition of property and fraud in the ever-

[8] In re VIA USA, Ltd. Telegroup, Inc. Disc. Call Int'l Co., 10 FCC Rcd. 9540 (1995), phone carriers challenged the practice of "uncompleted call signaling," by which competitors placed phone calls on lines that belong to other carriers to generate a "callback" from the reseller. Id. The practice circumvented higher telephone service prices charged in other countries. The Justice Department, in guidance provided to the FCC, indicated that this practice did not constitute wire fraud. Id. at 9544. They identified four elements that must be present for accessing phone service to constitute a scheme or artifice to defraud: "(1) the defendant obtained or conspired to obtain a service the carrier charged for; (2) the defendant avoided payment or did not pay the full rate for the service; (3) the defendant's conduct violated a statute, tariff or formal agreement; and (4) the conduct was unauthorized or was concealed." Id.

developing field of internet access, exceeds the bounds of the statute. In this context, the wire fraud statute is void for vagueness, and the charges must be dismissed.

V. VENUE SHOULD BE TRANSFERRED FOR THE CONVENIENCE OF THE PARTIES AND IN THE INTEREST OF JUSTICE

Alternatively, Harris asks this Court to transfer venue to the United States District Court for the District of Eastern District of California. "Upon the defendant's motion, the court may transfer the proceeding, or one or more counts, against that defendant to another district for the convenience of the parties and witnesses and in the interest of justice." Fed. R. Crim. P. 21(b).

Rule 21(b) gives a district court "broad discretionary power to transfer a criminal prosecution to another district." United States v. Muratoski, 413 F.Supp.2d 8, 9 (D.N.H. 2005). The Supreme Court and district courts in the First Circuit have identified ten factors that a judge considering a motion under Rule 21(b) should consider:

> (1) the location of the defendant; (2) the location of possible witnesses; (3) the location of events likely to be in issue; (4) the location of documents and records likely to be involved; (5) the disruption of defendant's business if the case is not transferred; (6) the expense to the parties; (7) the location of counsel; (8) the relative accessibility of the place of trial; (9) the docket condition of each district or division involved; and (10) any other special considerations relevant to transfer.

Id.

Harris and his family live in Oregon. It is a hardship for him to face trial on the opposite side of the country. The government asserts that a trial in Massachusetts is not a hardship because Harris would have to fly to the Eastern District of California and because he is a seasoned traveler. These assertions make light of the difference between a short flight within a time zone and a cross-country flight.[9] Additionally, it is an eight or nine hour drive from Harris's home to Sacramento, making driving an option. Harris's prior travel has nothing to do with his ability to prepare a defense and stand trial far from his friends and family.

Second, the potential witnesses who are likely to be in Massachusetts are the four users and any FBI agents who were involved in the case in Massachusetts. Keeping the case in Massachusetts because of these witnesses allows the government to control venue: three of the four users were located after indictment, and the government chose where to look for users. Additionally, there are potential witnesses on the West Coast: C.P. is alleged to live in California, TCNISO store employees are likely in California, and there were FBI agents involved in the case in California, including those who watched, visited, and searched the TCNISO store.

[9] In the same pleading in which the government asserts that it "is a plane ride either to Sacramento or Boston" from Oregon, it notes that a trial in Massachusetts would be convenient for them because "the DOJ prosecutor is in Washington, D.C., which is a one-hour shuttle away." Dkt. #42 at 12-13.

Third, the crux of activity at issue occurred in California. The overt acts that are alleged to have occurred in Massachusetts involve the actions of product users or the elective acts of the government. Many of the contested aspects of this case involve Harris's conduct and knowledge, and all of his actions are California-based.

Fourth, because TCNISO was based in California, it is likely that any documents not easily accessible in an electronic form are located there. Fifth, facing trial on the East Coast would significantly disrupt Harris's life and his ability to work. Sixth, facing trial across the country would impose a major emotional and financial toll on Harris and his family. Seventh, appointed counsel is available in California. Eighth, a trial in the Eastern District of California would be significantly more convenient for Harris, while moving the trial there is not likely to inconvenience the government. Ninth, statistics from the United States Courts website show that since 2009, the number of criminal filings in the Eastern District of California has decreased and the number of case terminations has increased. U.S. Courts, Federal Judicial Caseload Statistics, available at http://www.uscourts.gov/Viewer.aspx?doc=/uscourts/Statistics/FederalJudicialCaseloadStatistics/2010/tables/D00CMar10.pdf (last visited Jan. 21, 2011). The District of Massachusetts

has seen the same changes, indicating that docket conditions should not impede this transfer.

Finally, a major factor in favor of a discretionary transfer is the fact that the government has stated that it intends to file a case charging Harris with tax fraud in the Eastern District of California. The charges relate to TCNISO and its revenues and implicate some of the same discovery. If this case remains in this District, Harris will have to simultaneously defend himself against tax charges in the Eastern District of California. He will have to consult with two lawyers and deal with two courts defending two series of serious federal felonies.

For all of these reasons, Harris asks this Court to transfer venue to the Eastern District of California for the convenience of the parties and in the interest of justice.

VI. CONCLUSION

This Court should dismiss the indictment against Harris for lack of venue. The government cannot establish, by a preponderance of the evidence, that venue is proper in the District of Massachusetts. Further, the Court should dismiss on the merits because the wire fraud based charges are inadequate as a matter of pleading and unconstitutionally vague. In the alternative, this Court should transfer the

case to the Eastern District of California in the interests of justice.

RYAN HARRIS
By his attorney,

/s/ Charles P. McGinty

Charles P. McGinty
B.B.O. #333480
Federal Defender Office
51 Sleeper Street
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on August 4, 2011.

/s/ Charles P. McGinty

Charles P. McGinty